MATHEMATICS PROBLEM 142

All of the numbers in this problem and its solution are in the octal, or base 8, system. For example, $1234 = 1\times8^3 + 2\times8^2 + 3\times8^1 + 4\times8^0 = (668)_{10}$, where the subscript "10" indicates "668" is in base 10. (This problem is motivated by a comment of Professor Hanna on the e-mail correction to Math. Prob. 141.)

a. What are the last four octal digits of $3^{1234567}$?

b. What are the last four octal digits of $4^{1234567}$?

Show all work as if done "by hand" without computer. (You may use calculator for multiplication only.)

Each midshipman submitting a correct solution with a correct explanation to Problem 142 by 1700 Friday 12 November 2004 will be recognized as a solver on the next problem. Submit solutions to Prof. Wardlaw at mathprob@usna.edu (please no attachments!) or via his Math Dept mailbox in Preble Hall, second deck.

Midshipmen Jonathan Shaver submitted a correct solution to Math Problem 141. Midshipman Bill Lipstreu wrote a JAVA program that computed the correct answers.

A solution to Math Problem 141 is on the back of this page and is posted on the Math Dept bulletin board on the second floor of Preble Hall across from the stairs

MATHEMATICS PROBLEM 141

a. What are the last four digits of $3^{123456789}$?

b. What are the last four digits of $4^{123456789}$?

Show all work done "by hand" without computer. (You may use calculator for multiplication only.)

Solution

a. We quickly observe that we need only keep the last 4 digits in our calculations of powers of 3. Thus, $3^1 = 3$, $3^2 = 9$, $3^3 = 27$, $3^4 = 81$, $3^8 = 6561$, $3^{12} \equiv 1441$ (Here the symbol "≡" means "is congruent modulo 10000", and it is used to indicate that we are discarding all but the last 4 digits in our calculations.), $3^{16} \equiv 6721$, $3^{20} \equiv 4401$, $3^{40} \equiv 8801$, $3^{60} \equiv 3201$, $3^{80} \equiv 7601$, $3^{100} \equiv 2001$, $3^{200} \equiv 4001$, $3^{300} \equiv 6001$, $3^{400} \equiv 8001$, $3^{500} \equiv 0001$. It now follows that $3^{123456789} = (3^{123456500})(3^{289}) = (3^{500})^{246913}(3^{289}) \equiv (1^{246913})(3^{289}) = 3^{289} = (3^{200})(3^{80})(3^8)(3^1) \equiv (4001)(7601)(6561)(3) \equiv (1601)(6561)(3) \equiv (4161)(3) \equiv 2483 \bmod(10000)$. Hence, the last four digits of $3^{123456789}$ are **2483.**

b. Powers of 4 are a bit trickier: In some sense, the final digit 6 plays the role of the final digit 1 in part a. $4^1 = 4$, $4^2 = 16$, $4^4 = 256$, $4^6 = 4096$, $4^8 \equiv 5536$, $4^{10} \equiv 8576$, $4^{16} \equiv 7296$, $4^{20} \equiv 7776$, $4^{30} \equiv 6976$, $4^{50} \equiv 5376$, $4^{250} \equiv 9376$. Since $(9376)(16) \equiv 16$, it follows that $(9376)(4^k) \equiv 4^k$ for $k > 1$; that is, 9376 acts like 1 when multiplying powers of 4 greater than the first power. Hence, $4^{123456789} = (4^{250})^{493827}(4^{39}) \equiv (9376)(4^{39}) \equiv 4^{39} = (4^{30})(4^8)(4) \equiv (6976)(5536)(4) \equiv 6544$. Thus, the last four digits of $4^{123456789}$ are **6544.**

The following might help you understand the above solution and help in solving MathProb142:

Definition: For integers a, b, and m with $m > 1$, a is congruent to b modulo m, written $a \equiv b \pmod{m}$, if and only if $b - a = km$ for some integer k.

MP141 requires us to find the non-negative residue modulo $m = 10000 = 10^4$ of $a^N \pmod{m}$ for $a = 3$ or 4 and $N = 123456789$.

Euler's Totient Theorem. If a and $m > 1$ are relatively prime integers and ϕ is the Euler totient function given by $\phi(n) = n\Pi_{\text{Prime } p|n}(1 - 1/p)$, then

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Thus, $\phi(10000) = (10000)(1 - 1/2)(1 - 1/5) = 4000$ and $a^{4000} \equiv 1 \pmod{10000}$ whenever a has no factors in common with 10000. If we let (m) be the exponent of m, that is, the smallest positive integer k such that $a^k \equiv 1 \pmod{m}$ for all a relatively prime to m, we see that $(10^4) = \text{lcm}((2^4), (5^4)) = \text{lcm}(4, 500) = 500$ and $a^{500} \equiv 1 \pmod{10000}$ whenever $\gcd(a, 10) = 1$. (Actually, $(2) = 1$, $(4) = 2$, $(2^k) = 2^{k-2}$ for $k > 2$, $(p^k) = (2p^k) = (p-1)p^{k-1}$ for any odd prime p and any positive integer k, and $(mn) = \text{lcm}((m), (n))$ whenever $\gcd(m, n) = 1$.) Thus $(5^4) = 500$ implies that $4^{250} = 2^{500} \equiv 1 \pmod{5^4}$ and $4^{250} = 2^{500} \equiv 0 \pmod{2^4}$ explains why $4^{250} \equiv 9376 \pmod{10^4}$ acts like 1 when multiplying powers of 4 modulo 10000.